AMENDMENTS TO THE SPECIFICATION

Please amend the paragraph beginning on page 2, line 4 as follows:

[0003] A current ep station connects to the Internet by way of telephone circuits. However, high-speed Internet connection environments are becoming available in ordinary households due to the prevalence of high speed networks such as ADSL CATV, and optical fibers. Therefore, it is easily conceivable that next-generation machines for the ep station, with high-speed communication abilities, may appear.

Please amend the paragraph on page 4, line 22 to page 7, line 6 as follows:

[0010] In this case, an ~~encryption/decyption~~ encryption/decryption processing section 218 in the digital television device performs communications of various data in packet format with an ~~encryption/decyption~~ encryption/decryption processing section 204 of the network camera, via a communication processing section 216 of the digital television device itself, the Internet connection network, and a communication processing section 206 in the network camera. In order for the data-transmitting end and the data-receiving end to use the same encryption algorithm, the aforementioned negotiation is performed between the two ends. In a negotiation of an encryption algorithm, packets for the negotiation are exchanged with each ~~other~~ end. First, the encryption information determination section 214 of the digital television device generates a negotiation packet for transmission in a predetermined format, and proposes to the network camera an encryption algorithm to be used. At the network camera, the proposed encryption algorithm which has been obtained via the communication processing section 206 and the ~~encryption/decyption~~ encryption/decryption processing section 204 is passed to the encryption information determination section 202 as encryption/decryption information, and the encryption information determination section 202 determines whether the proposed encryption algorithm is usable. Then, a reply indicating the usability of the proposed encryption algorithm is given via the ~~encryption/decyption~~ encryption/decryption processing section 204 and the communication processing section 206. The encryption information determination section 214 in the digital television device receives this reply via the communication processing section 216 and the

2

~~encryption/decyption~~ encryption/decryption processing section 218, and if the received reply is "usable", it is notified, in the form of a negotiation packet, to the network camera that the proposed usable encryption algorithm is finalized; thus, the negotiation for the encryption algorithm to be used is ended. Moreover, the encryption information determination section 214 notifies the determined encryption algorithm to the ~~encryption/decyption~~ encryption/decryption processing section 218, and instructs this algorithm to be set. Furthermore, the encryption information determination section 202 also notifies the determined encryption algorithm to the ~~encryption/decyption~~ encryption/decryption processing section 204, and instructs this algorithm to be set. Next, the encryption information determination sections 214 and 202 and the ~~encryption/decyption~~ encryption/decryption processing sections 218 and 204 perform predetermined communications with each other, and, through a procedure which is determined in accordance with the set encryption algorithm, generate and set an encryption key and a decryption key of a predetermined format. Once the encryption key and the decryption key are generated, encrypted communications are enabled. An encrypted communication application 200 passes Video data which is imaged by an imaging section (not shown) to the ~~encryption/decyption~~ encryption/decryption processing section 204. By using the set encryption algorithm, the ~~encryption/decyption~~ encryption/decryption processing section 204 encrypts the video data, and sends it as data packets to the digital television device via the communication processing section 206 and the Internet connection network. At the digital television device, the data packets are received by the communication processing section 216 and thereafter decrypted by the ~~encryption/decyption~~ encryption/decryption processing section 218, and the decrypted video data is passed to the encrypted communication application 210. The encrypted communication application 210 performs a process of displaying the video data from the network camera, at a predetermined position and in a predetermined size on a display of the television device.

Please amend the paragraph beginning on page 9, line 16 as follows:

[0015] A communication device according to a first aspect of the present invention

comprises an encryption information determination section for selecting an encryption algorithm from among a plurality of previously provided encryption algorithms, the selected encryption algorithm being different depending on a predicted total used resource or an actual total used resource; an ~~encryption/decyption~~ encryption/decryption processing section for encrypting a packet in accordance with the encryption algorithm selected by the encryption information determination section; and a communication processing section for transmitting the packet encrypted by the ~~encryption/decyption~~ encryption/decryption processing section.

Please amend the paragraph beginning on page 10, line 2 as follows:

[0016] A communication device according to a second aspect of the present invention comprises: an encryption information determination section for selecting an encryption algorithm from among a plurality of previously provided encryption algorithms, the selected encryption algorithm being different depending on an encryption algorithm or encryption algorithms used for one or more packets received from a communication counterpart; an ~~encryption/decyption~~ encryption/decryption processing section for encrypting a packet to be transmitted to the communication counterpart in accordance with the encryption algorithm selected by the encryption information determination section; and a communication processing section for transmitting the packet encrypted by the ~~encryption/decyption~~ encryption/decryption processing section.

Please amend the paragraph beginning on page 16, line 13 as follows:

[0023] Next, the functions of the network camera 12 and the communication device 24 will be specifically described. The network camera 12 includes an imaging section 14, an ~~encryption/decyption~~ encryption/decryption processing section 16, an encryption information determination section 18, and a communication processing section 20. The encrypted communication application 200 as shown in FIG. 43 may be provided between the imaging section 14 and the ~~encryption/decyption~~ encryption/decryption processing section 16.

Please amend the paragraph on page 16, line 21 to page 17, line 11 as follows:

[0024] The communication device 24, which is a home appliance having a communication function and a video recording function, includes a reception section 26, a video recording application 28, a resource monitoring section 30, an encryption information determination section 32, a communication processing section 36, an ~~encryption/decyption~~ encryption/decryption processing section 38, and a network camera application 34. The component elements encircled with a broken line in FIG. 1, i.e., the video recording application 28, the resource monitoring section 30, the encryption information determination section 32, the communication processing section 36, the ~~encryption/decyption~~ encryption/decryption processing section 38, and the network camera application 34, are realized by software being executed by an internal CPU. In the present embodiment, it is assumed that the algorithm selection method according to the present invention is employed by the encryption information determination section 32 in the communication device 24.

Please amend the paragraph on page 17, line 23 to page 18, line 17 as follows:

[0027] Next, the operation of the system when displaying video from the network camera 12 on the display 40 will be described. This process is divided into a preprocess for performing an encrypted communication, and a process of actually causing the network camera application 34 to operate. The preprocess for performing an encrypted communication will be described later. First, an outline of the process of actually causing the network camera application 34 to operate will be described. First, in the network camera 12, the video data taken by the imaging section 14 is encrypted by the ~~encryption/decyption~~ encryption/decryption processing section 16. The communication processing section 20 sends the encrypted video data onto the Internet 22 as packets directed to the communication device 24. At the communication device 24, the communication processing section 36 receives the encrypted packets from the Internet 22, the ~~encryption/decyption~~ encryption/decryption processing section 38 decrypts them, and the network camera application 34 outputs the decrypted video data to the display 40. Then, the display 40 displays the video. In this manner, the video which has been taken by means of the

5

network camera 12 is displayed on the display 40.

Please amend the paragraph on page 18, line 18 to page 19, line 5 as follows:

[0028] Next, the preprocess for performing an encrypted communication will be described. As used herein, the preprocess is a process of negotiating an encryption algorithm to be used for the encrypted communication and what should be used as an encryption key and a decryption key between the encryption information determination section 18 in the network camera 12 and the encryption information determination section 32 in the communication device 24, and setting these parameters in the respective ~~encryption/decyption~~ encryption/decryption processing sections 16 and 38. Hereinafter, a negotiation performed for preventing the load of the processing to be performed by the internal CPU of the communication device 24 from exceeding the performance of the internal CPU as shown in FIG. 44 will be described.

Please amend the paragraph on page 19, line 6 to page 20, line 10 as follows:

[0029] FIG. 2 is a block diagram illustrating component elements of the communication device 24 that are involved in the negotiation. In order for the data-transmitting end and the data-receiving end to use the same encryption algorithm, the negotiation is performed between the two ends. The communication processing section 36 performs data packet communications with the counterparting communication processing section. During the encryption algorithm negotiation, packets for the negotiation are exchanged with the counterpart. When transmitting packets, a negotiation packet generation/interpretation section 48 generates a negotiation packet for transmission in a predetermined format in accordance with an instruction from an encryption algorithm selection section 42, and when receiving packets, interprets the content of a received negotiation packet and passes the acquired information to the encryption algorithm selection section 42. The encryption algorithm selection section 42 notifies the determined encryption algorithm to an encryption algorithm setting section 50, and instructs the algorithm to be set. The ~~encryption/decyption~~ encryption/decryption processing section 38 uses the set encryption algorithm to perform ~~datan~~ data encryption and decryption. The encryption algorithm selection

6

section 42 has a CPU utilization statistics memory 44 for storing CPU utilization rate information which was previously obtained from the resource monitoring section 30 or obtained at the time of the negotiation. In the present embodiment, the encryption algorithm selection section 42 performs encryption algorithm proposing and selecting processes while referring to an encryption process and used-resource table 46 and the CPU utilization rate information obtained from the resource monitoring section 30. The encryption process and used-resource table 46 will be described later.

Please amend the paragraph on page 20, line 11 to page 21, line 2 as follows:

[0030] In the present embodiment, after the encryption information determination section 32 generates a negotiation packet and encrypts it, the encrypted negotiation packet is transmitted via the communication processing section 36; however, other embodiments would also be possible. For example, after the encryption information determination section 32 generates a negotiation packet, the ~~encryption/decyption~~ encryption/decryption processing section 38 may encrypt the negotiation packet, and the encrypted negotiation packet may be transmitted via the communication processing section 36. Alternatively, for example, the encryption information determination section 32 may generate a negotiation packet; the ~~encryption/decyption~~ encryption/decryption processing section 38 may encrypt the negotiation packet; thereafter, the encrypted negotiation packet may be once sent back to the encryption information determination section 32; and the encryption information determination section 32 may transmit the encrypted negotiation packet via the communication processing section 36.

Please amend the paragraph on page 32, line 24 to page 33, line 5 as follows:

[0058] Next, in order to actually use the returned encryption algorithm, the responder sets the encryption algorithm in the ~~encryption/decyption~~ encryption/decryption processing section 38 (S405). On the other hand, the initiator receives the response packet from the responder (S413), and sets the returned encryption algorithm in the ~~encryption/decyption~~ encryption/decryption processing section 16 in the network camera 12 (S414).

Please amend the paragraph beginning on page 33, line 6 as follows:

[0059] Thereafter, the network camera 12 converts the video data imaged by the imaging section 14 into encrypted data by using the encryption function of the encryption algorithm that has been set in the ~~encryption/decyption~~ encryption/decryption processing section 16, and appends thereto an identifier of the encryption algorithm, or an identification ID of information SA, i.e., a so-called security association which specifies the encryption algorithm and keys, that are set in the encryption information determination section 18. Then, the encrypted data is sent out on the Internet 22 as packets, via the communication processing section 20. The communication processing section 36 of the communication device 24 receives the packets, and based on the appended identifier of the encryption algorithm, or the identification ID of SA, performs decryption by means the ~~encryption/decyption~~ encryption/decryption processing section 38 using the encryption algorithm that has been negotiated and agreed upon, and displays the resultant video data on the display 40.

Please amend the paragraph beginning on page 34, line 7 as follows:

[0061] First, the encryption information determination section 32 in the communication device 24 (hereinafter "initiator") ascertains encryption algorithms supported by the ~~encryption/decyption~~ encryption/decryption processing section 38 (set A) (S801). Then, the initiator waits for a request to start negotiation. A request to start negotiation is issued when starting an encrypted communication, after the lapse of a predetermined period of time from a previous negotiation, or when a negotiation start command is executed.

Please amend the paragraph beginning on page 35, line 3 as follows:

[0064] At the responder, encryption algorithms supported by the ~~encryption/decyption~~ encryption/decryption processing section 16 (set E) are previously ascertained (S811). Thereafter, when a proposal packet is received from the initiator (S812), it is determined whether the ~~encryption/decyption~~ encryption/decryption processing section 16 supports the proposed

encryption algorithm (i.e., whether the proposed encryption algorithm is contained in set E) (S813). If the proposed encryption algorithm is not supported by the encryption/decryption encryption/decryption processing section 16 (i.e., the proposed encryption algorithm is not contained in set E), a response cannot be returned to the initiator; therefore, the negotiation fails, and a next proposal packet is awaited. If the proposed encryption algorithm is supported by the encryption/decyption encryption/decryption processing section 16 (i.e., the proposed encryption algorithm is contained in set E), the encryption algorithm is returned to the initiator (S814), and the returned encryption algorithm is set in the encryption/decyption encryption/decryption processing section 16 (S815).

Please amend the paragraph beginning on page 35, line 20 as follows:

[0065] At the initiator, upon receiving the response packet (S804), the returned encryption algorithm is set in the encryption/decyption encryption/decryption processing section 38 (S805).

Please amend the paragraph beginning on page 39, line 20 to page 40, line 1 as follows:

[0074] First, the encryption information determination section 32 in the communication device 24 (hereinafter "responder") ascertains the encryption algorithms supported by the encryption/decyption encryption/decryption processing section 38 (set A) (S1001). Thus, it enters a state of waiting for a proposal packet from the encryption information determination section 18 in the network camera 12 (hereinafter "initiator").

Please amend the paragraph beginning on page 43, line 24 as follows:

[0086] Next, in order to actually use the returned encryption algorithm, the responder sets the encryption algorithm in the encryption/decyption encryption/decryption processing section 38 (S1005). On the other hand, the initiator receives a response packet from the responder (S1013), and sets the returned encryption algorithm in the encryption/decyption

9

encryption/decryption processing section 16 in the network camera 12 (S1014).

Please amend the paragraph beginning on page 44, line 9 as follows:

[0088] First, the encryption information determination section 32 in the communication device 24 (hereinafter "initiator") ascertains the encryption algorithms supported by the ~~encryption/decyption~~ encryption/decryption processing section 38 (set A) (S1201). Then, the initiator waits for a request to start negotiation. A request to start negotiation is issued when starting an encrypted communication, after the lapse of a predetermined period of time from a previous negotiation, or when a negotiation start command is executed.

Please amend the paragraph beginning on page 45, line 5 as follows:

[0091] At the responder, encryption algorithms supported by the ~~encryption/decyption~~ encryption/decryption processing section 16 (set E) are previously ascertained (S1211). Thereafter, when a proposal packet is received from the initiator (S1212), it is determined whether the ~~encryption/decyption~~ encryption/decryption processing section 16 supports the proposed encryption algorithm (i.e., whether the proposed encryption algorithm is contained in set E) (S1213). If the proposed encryption algorithm is not supported by the ~~encryption/decyption~~ encryption/decryption processing section 16 (i.e., the proposed encryption algorithm is not contained in set E), a response cannot be returned to the initiator; therefore, the negotiation fails, and a next proposal packet is awaited. If the proposed encryption algorithm is supported by the ~~encryption/decyption~~ encryption/decryption processing section 16 (i.e., the proposed encryption algorithm is contained inset E), the encryption algorithm is returned to the initiator S1214), and the returned encryption algorithm is set in the ~~encryption/decyption~~ encryption/decryption processing section 16 (S1215).

Please amend the paragraph beginning on page 45, line 22 as follows:

[0092] At the initiator, upon receiving the response packet (S1204), the returned encryption algorithm is set in the ~~encryption/decyption~~ encryption/decryption processing section

10

38 (S1205).

Please amend the paragraph beginning on page 47, line 5 as follows:

[0098] First, the encryption information determination section 32 ascertains the encryption algorithms supported by the ~~encryption/decyption~~ encryption/decryption processing section 38 (set A) (S1401). Moreover, the encryption information determination section 18 ascertains the encryption algorithms supported by the ~~encryption/decyption~~ encryption/decryption processing section 16 (set E) (S1421).

Please amend the paragraph beginning on page 49, line 8 as follows:

[0103] Next, the responder transmits a response packet in response to the received proposal packet (S1423 to S1425), and sets the returned encryption algorithm to the ~~encryption/decyption~~ encryption/decryption processing section 16 (S1426). Upon receiving the response packet (S1406), the initiator sets the returned encryption algorithm to the ~~encryption/decyption~~ encryption/decryption processing section 38 (S1407). The above procedure (S1406, S1407, S1423 to S1426) is exactly the same as that in the case where the communication device 24 works as an initiator in Embodiment 1 (S804, S805, S812 to S815 in FIG. 8), and any detailed descriptions thereof are omitted.

Please amend the paragraph beginning on page 54, line 8 as follows:

[0118] <operation procedure of the counterparting end>

Next, the operation procedure of the counterparting end will be described. First, the counterparting end performs an encryption algorithm negotiation with the encryption algorithm selecting-end (S1621). At this time, a plurality of encryption algorithms are agreed upon between itself and the encryption algorithm selecting-end, and encryption keys and decryption keys for all such encryption algorithms are generated. Then, it is determined whether an encrypted packet has been received from the communication device 24 (S1622). If the result of the determination is YES, the encryption algorithm which is applied to this packet is set as the encryption algorithm

11

to be used in the ~~encryption/decyption~~ encryption/decryption processing section 16 (S1623).

Please amend the paragraph beginning on page 54, line 21 as follows:

[0119] Next, it is checked whether a packet transmission request has been issued (S1624). If a packet transmission request has been issued, packets for transmission are encrypted by using the encryption algorithm which has been set at step S1623, and are transmitted (S1625).

Please amend the paragraph beginning on page 60, line 1 as follows:

[0130] The ~~encryption/decyption~~ encryption/decryption processing section 80, which comprises a plurality of encryption algorithm processing means (or programs for executing encryption algorithm processing procedures), performs processing of negotiation packets, generation of keys, disclosed values, public keys, secret keys, and shared keys used for encryption/decryption, encryption of data to be transmitted, decryption of received data, and the like.

Please amend the paragraph beginning on page 60, line 8 as follows:

[0131] The communication processing section 78 transmits packets which are generated by the ~~encryption/decyption~~ encryption/decryption processing section 80 onto an Internet connection network in predetermined communication protocol format, and extracts packets from data in communication protocol format which are received from the Internet connection network and passes them to the ~~encryption/decyption~~ encryption/decryption processing section 80.

Please amend the paragraph beginning on page 61, line 15 as follows:

[0136] Next, the operation of the system when displaying video from a network camera on a display will be described. This process is split into two processes: preprocess for performing encrypted communications and a process of actually running a network camera application. The preprocess for performing encrypted communications will be described later. First, an outline of the process of actually running a network camera application will be described. The processing at

12

the network camera side has been described with reference to FIG. 43 and in Embodiment 1 (FIG. 1), and the descriptions thereof are omitted here. In the communication device shown in FIG. 18, encrypted packets based on video data is received from the Internet connection network by the communication processing section 78, decrypted by the ~~encryption/decyption~~ encryption/decryption processing section 80, and the decrypted video data is passed to the encrypted communication application 70, which outputs the video data at a predetermined position and in a predetermined size on a display (not shown) . Then, the display displays the video. In this manner, video which has been taken by the network camera is displayed on the display.

Please amend the paragraph beginning on page 64, line 2 as follows:

[0140] The encryption information determination section 74 includes an encryption process and used-resource table 76 in itself. An example of the encryption process and used-resource table 76 is shown in FIG. 20. In FIG. 20, for two kinds of encryption algorithms (DES-CBC, 3DES-CBC) held in the ~~encryption/decyption~~ encryption/decryption processing section 80, their respective used resource amounts, i.e., average used CPU resource (unit: MIPS/Mbps), average used memory resource (MB), and encryption strengths (indicated in terms of order) are stored. In this example, one unit average used CPU resource indicates the CPU resource necessary for performing encryption/decryption for a data transfer amount of 1 Mbps. As there is more data transfer amount, more encryption/decryption resource is proportionally required. It is indicated that CPU resources of 100 MIPS and 300 MIPS are respectively consumed when transferring 1 Mbps of data.

Please amend the paragraph on page 69, line 1 to page 70, line 14 as follows:

[0149] As a preprocess for encrypted communications, the ~~encryption/decyption~~ encryption/decryption processing section 80 performs a negotiation with the ~~encryption/decyption~~ encryption/decryption processing section 204 in the network camera shown in FIG. 43 (which is the communication counterpart) in order to generate a shared key required

13

for encrypted communications, and generates the shared key according to specifications such as Diffie-Hellman, IKE, or IPsec. Once the generation of the shared key is completed in both ~~encryption/decyption~~ encryption/decryption processing sections 80 and 204, the ~~encryption/decyption~~ encryption/decryption processing section 80 in the communication device notifies to the encrypted communication application 70 that encrypted communications are ready to be performed, and the ~~encryption/decyption~~ encryption/decryption processing section 204 in the network camera notifies to the encrypted communication application 200 that encrypted communications are ready to be performed. Upon receiving this notification, the encrypted communication application 200 sends video data from the camera to the ~~encryption/decyption~~ encryption/decryption processing section 204; the ~~encryption/decyption~~ encryption/decryption processing section 204 encrypts this video data by using DES-CBC; and the communication processing section 206 generates encrypted packets of video data and sends the packets to the communication processing section 78 via the Internet connection network. The ~~encryption/decyption~~ encryption/decryption processing section 80 gets the received data from the communication processing section 78 and performs decryption of the coding, and passes the video data to the encrypted communication application 70. As already described above, the encrypted communication application 70 displays the video on the display. When the schedule section 64 detects that the current time has reached 12:00 by referring to its internal clock, the schedule section 64 activates task a (i.e., the application 60) while continuing task b, in accordance with the event and used-resource table 68. At 12:30, task c is also activated. At 13:00, task a is stopped. At 13:30, task c is stopped. Thus, at each event time, the content of the row of that event time is compared against the content of the row of the immediately previous event time, and any additional task or encryption algorithm from the previous row is activated, and any task or encryption algorithm from the previous row which is no longer described is stopped.

Please amend the paragraph on page 71, line 10 to page 72, line 3 as follows:
[0152] The values of used resource amounts for tasks a, b, and c, e.g., average used CPU

resource, average used memory resource, and average data transfer amount may be previously stored in the application 60 or the encrypted communication application 70 at the time of manufacture or shipment of the communication device, or they may be stored to the application 60 or the encrypted communication application 70 at the time when each application program is externally downloaded via the Internet connection network or TV data broadcast. The average used CPU resource, average used memory resource, order of encryption strengths, the number of preprocess instructions (described later) , and the like for each encryption algorithm may be stored as encryption/decryption information in a table which is provided in the ~~encryption/decyption~~ encryption/decryption processing section 80. In this case, the encryption information determination section 74 reads such encryption/decryption information and writes it to the encryption process and used-resource table 76. Alternatively, it may be previously stored in the encryption process and used-resource table 76.

Please amend the paragraph on page 73, line 7 to page 74, line 24 as follows:

[0155] FIG. 23 shows an exemplary hardware structure of a communication device which performs the aforementioned process. In FIG. 23, a CPU 94, a ROM 96, a RAM 98, an HDD 104, and a modem 116 are coupled to a bus line which constitutes transfer means 92. Such a structure is a standard computer system structure. In the ROM 96, a program for system boot and data which does not need to be updated are stored. An area 106 in the HDD 104 stores a control program,. e.g. , operating system (OS) , for managing the overall system and performing various controls, a resource monitoring section program for allowing the CPU 94 to function as the resource monitoring section 82, and a communication processing section program for allowing the CPU 94 to function as the communication processing section 78. An area 108 stores a schedule section program for allowing the CPU 94 to function as the schedule section 64 and an encryption information determination section program for allowing the CPU 94 to function as the encryption information determination section 74. An area 110 stores an ~~encryption/decyption~~ encryption/decryption processing section program for allowing the CPU 94 to function as the ~~encryption/decyption~~ encryption/decryption processing section 80 and encryption algorithm

15

programs. An area 112 stores application programs and encrypted communication application programs. A file portion in an area 114 stores data of recorded TV programs. A transport stream of TV programs received by an antenna 84 and a tuner 86 is decoded by the CPU 94 in accordance with the application 60 which has been loaded into the RAM 98 from the area 112, and the decoded results are stored (recorded) in the file portion of the area 114. The recorded data is read after a predetermined time shift period, and subjected to an AV decoding by the CPU 94. The decoded audio data and video data are output as an audio output and a video output via an audio processing 88 and a display processing 90. Preprogramming information which is instructed by operating a remote control 102 is received by the schedule section program via a remote control IF (interface) 100, and is registered by the schedule section program to the schedule and used-resource table 66. Thereafter, in accordance with the control program, the CPU 94 sequentially loads the schedule section program, the encryption information determination section program, the ~~encryption/decyption~~ encryption/decryption processing section program, the encryption algorithm programs, application programs, the encrypted communication programs, the resource monitoring section program, and the communication processing section program onto the RAM 98, and performs the above-described processes in accordance with the respective programs.

Please amend the paragraph beginning on page 77, line 9 as follows:

[0161] Once Mt is determined, the schedule section 64 changes the start time of task b in the event and used-resource table 68 so as to be earlier by Mt (sec.). By doing so, task b of the encrypted communication application 70 is activated Mt (sec.) before 11:45. Therefore, it becomes possible to perform an actual encrypted communication by the encrypted communication application 70 when it is Mt (sec.) after the completion of the preprocess, e., 11: 45. Specifically, an event indicating the start of a preprocess for task b may be additionally inserted at a time which is Mt earlier than the start event time of task b, and the schedule section 64 may instruct the ~~encryption/decyption~~ encryption/decryption processing section 80 to 20 start the preprocess Mt (sec.) before 11:45, and task b may be activated at 11:45, by which time the

preprocess has been completed.

Please amend the paragraph on page 79, line 5 to page 80, line 19 as follows:

[0167] Referring to FIG. 21 or FIG. 22, in the slot (11:45-12:00) and the slot (13:00-unknown), those encryption algorithms whose CPU resource does not exceed a tolerable used CPU resource Kcpu (MIPS) of 500 MIPS, i.e., whose CPU utilization rate does not exceed a tolerable limit of 50%, are 3DES-CBC and DES-CBC, but the former is higher in encryption strength. Based on the event and used-resource table 68 shown in FIG. 22A and FIG. 22B, for each event slot, the schedule section 64 notifies to the encryption information determination section 74 an encryption algorithm which does not allow the total used resource to exceed the tolerable used CPU resource Kcpu (MIPS)=500 MIPS. In the case where a plurality of encryption algorithms have been notified, the encryption information determination section 74 selects one that has the highest encryption strength, and notifies the selected encryption algorithm to the schedule section 64. For each event time and for each encryption algorithm in the event and used-resource table 68, there is newly provided a selection registering column (not shown) which indicates whether that encryption algorithm has been selected. In a selection registering column for the encryption algorithm that has been notified from the encryption information determination section 74, the schedule section 64 writes a selection code indicating that that encryption algorithm has been selected. Next, as in the case of Embodiment 6, the schedule section 64 calculates (tolerable used CPU resource -total used resource) = CPU resource margin Ycpu (MIPS) in a time zone before an event time at which to switch encryption algorithms, determines Mt (sec.) = Im/Ycpu, and inserts a preprocess event at Mt (sec.) before this event time. After generating such event and used-resource tables 68 (one corresponding to DES-CBC and another corresponding to 3DES-CBC), the schedule section 64 controls the activation/execution/stopping of each application and a preprocess and code processing and the like for an encryption algorithm to be used next, by referring to these event and used-resource tables 68. At this point, by referring to the selection code in the selection registering column in the event and used-resource table 68, the schedule section 64 causes the ~~encryption/decyption~~ encryption/decryption processing section

17

80 to perform a preprocess and encryption/decryption processes for the selected encryption algorithm.

Please amend the paragraph on page 84, line 17 as follows:

[0179] In the present embodiment, as an ~~encryption/decyption~~ encryption/decryption processing section 80, that which is capable of executing a given encryption algorithm and a preprocess for another encryption algorithm in parallel is provided.

Please amend the paragraph beginning on page 114, line 1 as follows:

[0229] In the structure shown in FIG. 18, encryption/decryption information is exchanged between the encryption information determination section 74 and the ~~encryption/decyption~~ encryption/decryption processing section 80. Alternatively, the encryption information determination section 74 may exchange with the encrypted communication applications 70 and 72 encryption/decryption information corresponding to that encrypted communication application, and the encrypted communication applications 70 and 72 may exchange with the ~~encryption/decyption~~ encryption/decryption processing section 80 encryption/decryption information corresponding to the encrypted communication application themselves.

Please amend the paragraph beginning on page 114, line 19 as follows:

[0231] In the structure of FIG. 18, the encryption information determination section 74 and the ~~encryption/decyption~~ encryption/decryption processing section 80 may be composed as a single block which handles the encryption process and used-resource table 76 and the encryption/decryption information and exchanges relevant information with the schedule section 64 or the encrypted communication applications 70 and 72.

Please amend the paragraph beginning on page 118, line 16 as follows:

[0242] FIG. 36 is a functional block diagram illustrating the structure of the communication device 120. In FIG. 36, the communication device 120 comprises an encrypted

communication application 128, an encryption information determination section 130, an ~~encryption/decyption~~ encryption/decryption processing section 136, and an communication processing section 138. The encryption information determination section 130 holds an encryption process and used-resource table 132 and an encryption algorithm statistics table 134.

Please amend the paragraph on page 119, line 21 to page 120, line 13 as follows:

[0245] FIG. 39 is a functional block diagram illustrating the structure of the communication counterpart 122. In FIG. 39, the communication counterpart 122 (communication counterpart 122) comprises an encrypted communication application 140, a resource monitoring section 142, a communication processing section 144, ~~encryption/decyption~~ encryption/decryption processing section 146, and an encryption information determination section 148. The encryption information determination section 148 holds an encryption process and used-resource table 150. The functions of the resource monitoring section 142, the communication processing section 144, and the ~~encryption/decyption~~ encryption/decryption processing section 146 are similar to those described in FIG. 1. Moreover, the CPU utilization statistics memory 150 and the encryption process and used-resource table 152 are similar to those shown in FIG. 2. Since the communication counterparts 124 and 126 are similar in structure and operation to the communication counterpart 122, the descriptions of the communication counterparts 124 and 126 are omitted.

Please amend the paragraph on page 120, line 25 to page 121, line 20 as follows:

[0247] First, the operation of the communication device 120 when receiving a packet will be described. The communication processing section 138 receives an encrypted packet from the communication counterpart via a network, and passes the received encrypted packet to the ~~encryption/decyption~~ encryption/decryption processing section 136. The ~~encryption/decyption~~ encryption/decryption processing section 136 analyzes this encrypted packet, and extracts an identifier for identifying an encryption algorithm and a set of encryption/decryption keys used for this encrypted packet (hereinafter referred to as "first identifier") . The ~~encryption/decyption~~

19

encryption/decryption processing section 136 passes to the encryption information determination section 130 the first identifier and an identifier for identifying a communication counterpart of the communication device from which the encrypted packet was transmitted (hereinafter referred to as "second identifier") . Based on the first identifier received from the ~~encryption/decyption~~ encryption/decryption processing section 136, the encryption information determination section 130 identifies the encryption algorithm and the set of encryption/decryption keys, and passes these to the ~~encryption/decyption~~ encryption/decryption processing section 136. Moreover, based on the identified encryption algorithm and the set of encryption/decryption keys, and the second identifier received from the ~~encryption/decyption~~ encryption/decryption processing section 136, the encryption information determination section 130 updates the encryption algorithm statistics table 134. By using the encryption algorithm and the set of encryption/decryption keys received from the encryption information determination section 130, the ~~encryption/decyption~~ encryption/decryption processing section 136 decrypts the encrypted packet, and passes the packet which has thus been converted to plaintext to the encrypted communication application 128.

Please amend the paragraph on page 121, line 21 to page 122, line 19 as follows:

[0248] Next , the operation of the communication device 120 when transmitting a packet will be described. The encrypted communication application 128 generates a plaintext packet to be transmitted to the communication counterpart, and passes it to the ~~encryption/decyption~~ encryption/decryption processing section 136. The ~~encryption/decyption~~ encryption/decryption processing section 136 extracts the second identifier from the packet received from the encrypted communication application 128, and passes it to the encryption information determination section 130. Based on the second identifier received from the ~~encryption/decyption~~ encryption/decryption processing section 136, the encryption information determination section 130 selects an encryption algorithm by referring to the encryption process and used-resource table 132 and the encryption algorithm statistics table 134. The details of this encryption algorithm selection process will be described later. The encryption information determination

20

section 130 passes the selected encryption algorithm to the ~~encryption/decyption~~ encryption/decryption processing section 136. The ~~encryption/decyption~~ encryption/decryption processing section 136 encrypts the packet according to the encryption algorithm received from the encryption information determination section 130, and passes the encrypted packet to the communication processing section 138. The communication processing section 138 transmits the packet received from the ~~encryption/decyption~~ encryption/decryption processing section 136 to the communication counterpart via a network.

Please amend the paragraph beginning on page 127, line 2 as follows:

[0259] In the case where this method is adopted, the encryption information determination section 130 needs to update the "frequency" column in the encryption algorithm statistics table 134 shown in FIG. 38 each time ~~receiving~~ an encrypted packet is received. For example, in the case where an encryption algorithm is to be selected by taking into consideration the packets which were received in last five minutes, a history corresponding to five minutes is always retained in the "frequency" column of the encryption algorithm statistics table 134. With this method, the "last" column in the encryption algorithm statistics table 134 is unnecessary.

Please amend the paragraph beginning on page 132, line 13 as follows:

[0274] On the other hand, in the case where there are packets to be transmitted to the communication counterpart 122 (YES in S1624) , the encryption information determination section 130 selects one encryption algorithm from set F by using a method such as methods (1) to (6) above (S4002). Then, the ~~encryption/decyption~~ encryption/decryption processing section 136 encrypts the packet by using the encryption algorithm which has been selected by the encryption information determination section 130 (S4003).

Please amend the paragraph on page 134, line 16 to page 135, line 5 as follows:

[0279] FIG. 41 is a functional block diagram illustrating the structure of the communication device according to Embodiment 19. In FIG. 41, the communication device 154

21

comprises a resource monitoring section 156, an encrypted communication application 158, an encryption information determination section 160, an ~~encryption/decyption~~ encryption/decryption processing section 168, and a communication processing section 170. The encryption information determination section 160 holds a CPU utilization statistics memory 162, an encryption process and used-resource table 164, and an encryption algorithm statistics table 166. Since the structure and operation shown in FIG. 41 are similar to those shown in FIG. 36 or FIG. 39 except for the operation of the encryption information determination section 160, the descriptions thereof are omitted. The operation of the encryption information determination section 160 will be described later.

Please amend the paragraph on page 135, line 6 to page 136, line 1 as follows:

[0280] In the case where communications are performed between two communication devices, if both communication devices function as "primaries" or both function as "subordinates", the desirable effect in Embodiment 18 cannot be obtained. The reason is that, in the case where two communication devices both function as "primaries", it may be possible that, although the CPU utilization rate of one communication device is high, the other communication device may encrypt packets using a high-load encryption algorithm. In the case where two communication devices both function as "subordinates", an encryption algorithm which was first used by one of the communication devices may perpetually be used by both communication devices. Therefore, in the case where communications are performed between two communication devices, it is preferable that one of the communication devices functions as a "primary", while the other communication device functions as a "subordinate". Furthermore, it is preferable that one of the communication ~~device~~ devices that has relatively plenty CPU performance or the like functions as a "subordinate" because the communication device function as a "subordinate" always needs to use an encryption algorithm having a load which is conformed to its counterpart, irrespective of its own CPU utilization rate.

Please amend the paragraph on page 138, line 22 to page 139, line 23 as follows:

22

[0287] A second method is a method in which the performances of both are compared, so that the one having the lower performance is made "primary" and the one having the higher performance is made "subordinate". In this case, the encryption information determination section of communication device Y first notifies the performance of communication device Y (e.g., ability of the hardware such as the CPU, values which are set in the system, or the CPU resource which is available for encrypted communications as based on information at that point or at a past point) is notified to communication device X. Upon receiving this notification, the encryption information determination section of communication device X compares the performance of communication device X and the performance of communication device Y so as to determine which one of communication device X or communication device Y becomes "primary" or "subordinate" . Then, the result of the determination is notified to communication device Y. Thus, the primary-subordinate negotiation is ended. Alternatively, communication device X may notify performance to communication device Y, and communication device Y may determine which one of communication device X or communication device Y becomes "primary" or "subordinate". In this case, the notification of the performance from communication device X to communication device Y may be made concurrently with the aforementioned notification to communication device Y as to whether: communication device X can only be a "primary"; communication device X can only be a "subordinate" ; or communication device X can be either a "primary" or a "subordinate".

Please amend the paragraph beginning on page 141, line 14 as follows:

[0291] Moreover, the encryption/decyption encryption/decryption processing section may generally comprise one or more protocols for realizing encrypted communications such as IPsec, SSL, or TLS, and one or more programs based on a protocol for performing key information acquisition such as IKE (according to IKE , key information is acquired through a shared key exchanging; IKE realizes key 20 exchanging using Diffie-Hellman algorithm), and perform encrypted communications by calling an encryption algorithm such as DES-CBC, 3DES-CBC, or AES.